

**MANAGEMENT METHOD FOR MEDICAL TREATMENT INFORMATION
AND AREA MEDICAL TREATMENT INFORMATION SYSTEM**

Patent Number: JP11338950
Publication date: 1999-12-10
Inventor(s): BAN HIDEYUKI; OSAKI TAKANOBU; MATSUO HITOSHI
Applicant(s): HITACHI LTD
Requested Patent: ☐ JP11338950
Application Number: JP19980148714 19980529
Priority Number(s):
IPC Classification: G06F19/00; G06F17/60
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To make the medical treatment information of a patient possible to be offered to another institution by obtaining the consent of the patient himself/herself.

SOLUTION: This management method of the medical treatment information is provided with an offering destination authentication step 42 for confirming the propriety of offering destination, an offering origin consent confirmation step 43 for confirming the manager (doctor) of the medical treatment information relating to the offering of the medical treatment information, a patient consent confirmation step 44 for confirming the consent of the patient himself/ herself and a medical treatment information access permission step 45 for offering the medical treatment information in the case of confirming the consent of both of the manager and the patient. Thus, patient's privacy relating to the medical treatment information is protected.

Data supplied from the esp@cenet database - I2

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-338950

(43)公開日 平成11年(1999)12月10日

(51)Int.Cl.⁸
G 0 6 F 19/00
17/60

識別記号

F I
G 0 6 F 15/42
15/21
H
3 6 0

審査請求 未請求 請求項の数5 O L (全 9 頁)

(21)出願番号 特願平10-148714

(22)出願日 平成10年(1998)5月29日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 伴 秀行

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(72)発明者 大▲崎▼ 高伸

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(72)発明者 松尾 仁司

東京都国分寺市東恋ヶ窪一丁目280番地

株式会社日立製作所中央研究所内

(74)代理人 弁理士 小川 勝男

(54)【発明の名称】 診療情報の管理方法及びこれを用いた地域医療情報システム

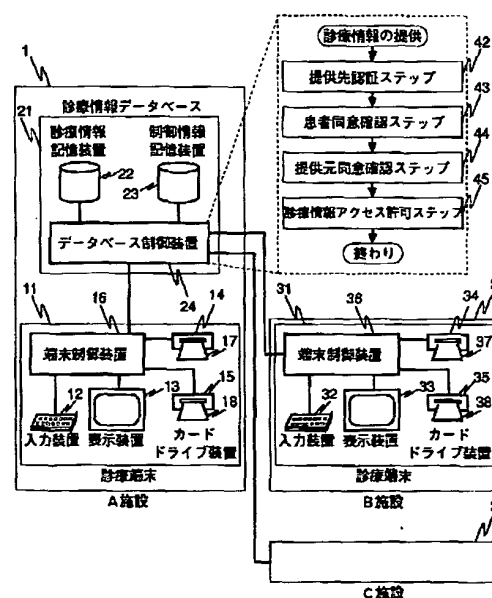
(57)【要約】

【課題】 患者の診療情報を患者本人の同意を得て他施設に提供する診療情報の管理方法及びこれを用いた地域医療情報システムを提供する。

【解決手段】 提供先の正当性を確認する提供先認証ステップ42と、診療情報を提供に関する診療情報の管理者(医師)の同意を確認する提供元同意確認ステップ43と、患者自身の同意を確認する患者同意確認ステップ44と、管理者と患者の両方の同意を確認した場合に診療情報を提供する診療情報アクセス許可ステップ45とを備える。

【効果】 診療情報に関する患者プライバシーを保護できる。

図1



【特許請求の範囲】

【請求項1】診療施設で受診した患者の診療情報を前記診療施設とは異なる他の診療施設に提供する診療情報の管理方法に於いて、前記他の診療施設の正当性を確認して認証する提供先認証ステップと、前記診療施設の診療情報の管理者が、前記患者の診療情報を前記他の診療施設に提供することを同意したことを確認する提供元同意確認ステップと、前記患者自身が、前記患者の診療情報を前記他の診療施設に提供することを同意したことを確認する患者同意確認ステップと、前記提供元同意確認ステップと前記患者同意確認ステップの確認結果を用いて、前記管理者と前記患者自身の両方の同意を確認した場合に、前記患者の診療情報を前記他の診療施設に提供することを許可する診療情報アクセス許可ステップとを有することを特徴とする診療情報の管理方法。

【請求項2】請求項1記載の診療情報の管理方法に於いて、前記提供元同意確認ステップと前記患者同意確認ステップの確認結果を保存する同意記録ステップを有し、前記診療情報アクセス許可ステップは、前記同意記録ステップで保存された確認結果を用いて、前記患者の診療情報を前記他の診療施設に提供することを特徴とする診療情報の管理方法。

【請求項3】請求項1又は請求項2に記載の診療情報の管理方法に於いて、前記提供元同意確認ステップ及び前記患者同意確認ステップは、確認に必要な情報を提供元の前記診療施設以外から伝送して行うことを特徴とする診療情報の管理方法。

【請求項4】請求項1から請求項3の何れかに記載の診療情報の管理方法に於いて、前記管理者の同意を確認した結果を、可搬型記録媒体に記録する媒体書き込みステップと、前記媒体書き込みステップで記録された確認結果を読み出す媒体読み出しステップとを有し、前記提供元同意確認ステップは、前記媒体読み出しステップで読み出した確認結果を用いて同意したことを確認することを特徴とする診療情報の管理方法。

【請求項5】診療施設に於いて受診した患者の診療情報を他の診療施設に提供する地域医療情報システムに於いて、請求項1から請求項4の何れかに記載の診療情報の管理方法を用いることを特徴とする地域医療情報システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、病院、診療所、検査センタ等の診療施設に於いて受診した患者の診療情報を他の診療施設に提供する診療情報の管理方法及びこれを用いた地域医療情報システムに関する。

【0002】

【従来の技術】従来技術の例として、「JIS型ICカードを用いた安全な医療情報通信システム—基本機能の検証—」(MEDICAL IMAGING TECH

NOLOGY、Vol. 15、No. 4、第451～452頁)に、デジタル化された画像、カルテ、検査データ等の診療情報を他の診療施設に伝送する方法が記載されている。この従来技術では、施設又は各個人がICカードを所持し、ICカードに記録された鍵を互いに確認して患者の診療情報を安全に伝送している。

【0003】

【発明が解決しようとする課題】上記従来技術では、診療情報に関する患者プライバシー(患者の診療情報を患者自身が制御すること)は考慮されていなかった。従って、患者の診療情報は、患者本人への同意なく、受診した診療施設や医師の意志や判断のみにより、他の病院、診療所等の診療施設、生命保険会社、信用調査機関等の関連会社に提供される怖れがあるという問題があった。

【0004】本発明の目的は、上記問題を解決し、診療情報を他の診療施設に提供する際に、患者プライバシーの侵害を防止可能な診療情報の管理方法及びこれを用いた地域医療情報システムを提供することにある。

【0005】

【課題を解決するための手段】本発明の診療情報の管理方法では、診療施設で受診した患者の診療情報(以下の説明では、「患者の診療情報」を単に「診療情報」、「患者Xの診療情報」を単に「診療情報X」と略記する。)を他の診療施設に提供する際、他の診療施設の正当性を確認して認証する提供先認証ステップと、診療施設の診療情報の管理者が、診療情報を認証した他の診療施設に提供することを同意したことを確認する提供元同意確認ステップと、患者自身が、診療情報を認証した他の診療施設に提供することを同意したことを確認する患者同意確認ステップと、提供元同意確認ステップと患者同意確認ステップの確認結果を用いて、管理者と患者自身の両方の同意を確認した場合に、診療情報を認証した他の診療施設に提供する診療情報アクセス許可ステップとを有することに特徴がある。更に、提供元同意確認ステップと患者同意確認ステップの確認結果を保存する同意記録ステップを有し、診療情報アクセス許可ステップは、同意記録ステップで保存された確認結果を用いて、患者の診療情報を他の診療施設に提供すること、提供元同意確認ステップ及び患者同意確認ステップは、確認に必要な情報を提供元の診療施設以外から伝送して行うこと、管理者の同意を確認した結果を、可搬型記録媒体に記録する媒体書き込みステップと、媒体書き込みステップで記録された確認結果を読み出す媒体読み出しステップとを有し、提供元同意確認ステップは、媒体読み出しステップで読み出した確認結果を用いて同意したことを確認することにも特徴がある。本発明の地域医療情報システムは、上記診療情報の管理方法を使用することに特徴がある。

【0006】

【発明の実施の形態】以下、本発明の実施例を、図面を

用いて詳細に説明する。なお、先に述べたように、「患者の診療情報」を単に「診療情報」、「患者Xの診療情報」を単に「診療情報X」と略記する。

【0007】(第1の実施例)図1は、A施設1、B施設2、C施設3との間で診療情報を共有する第1の実施例の地域医療情報システムを説明する図である。第1の実施例では、特にA施設1に診療端末11が、B施設2に診療端末31が配置され、A施設からB施設に診療情報を提供する手順を例にとり説明する。図1に於いて、各施設の診療端末11、31は、キーボードやマウス等の入力装置12、32、CRT等の表示装置13、33、ICカード17、18、37、38をセットするカードドライブ装置14、15、34、35、診療情報データベース21との間で診療情報のアクセス(読み書き)及び診療端末全体を制御する端末制御装置16、36を備える。

【0008】A施設は、A施設で受診した診療情報を管理する診療情報データベース21を備える。診療情報データベース21は、診療情報を格納する診療情報記憶装置22、診療情報データベース21に格納された診療情報の管理に必要な情報を記録する制御情報記憶装置23、施設内及び施設外からの診療情報のアクセス及び診療情報データベース全体を制御するデータベース制御装置24を備える。A施設とB施設とは離れており、診療情報データベース21とB施設の診療端末31との間は、例えば電話回線等を用いたネットワークで結ばれている。

【0009】ICカード17、18、37、38は、第1の実施例の地域医療情報システムの利用者(即ち、施設で受診した患者本人、及び診療情報の管理者)に配布され、本人確認に用いられる。診療情報の管理者は、例えば、施設毎に予め割り当てた診療情報管理の担当者、又は患者の診療を行う医師自身である。診療所等の小規模の施設では、診療を行う医師自身が管理者を兼ね、複数の医師が勤務する病院では、患者を診療する各医師が院内の診療情報管理の担当者を代行し管理者を兼ねる場合がある。以下の説明では、管理者は各施設の医師自身とする。

【0010】以下、図1に示す構成を用いて、A施設で受診した患者XをB施設に紹介する際、A施設(医師F)で発生した診療情報XをB施設(医師G)に提供する例をとり説明する。まず、A施設で診療情報Xを診療情報データベースに記録する。診療端末11は、診療に先立って利用者の医師の本人確認を行う。医師Fは自分のICカード17をカードドライブ装置14にセットし、入力装置12から暗証番号を入力する。端末制御装置16は、入力された暗証番号と予めICカード上に記録された暗証番号とが一致する時、利用者が医師F本人であると判断し、診療端末11を利用可能とする。

【0011】患者Xの診療を行う場合、診療端末11を

用いて、患者に対しても医師と同様に本人確認を行う。例えば、患者のICカード18とカードドライブ装置15とを用いて、医師Fと同様な手順により行う。医師Fは問診や触診等を行い、患者の既往症や主訴等の基本的な診療情報を取得し、各種検査(生化学検査や画像診断等)、薬の投与等の適当な処置を施す。診察や処置の内容、その他診療を進める中で発生する経過記録や要約(カルテ記載内容に相当)等は、検査装置から診療情報データベースに直接伝送するか、医師Fが入力装置12を操作する等して入力される。この入力内容は、端末制御装置16、データベース制御装置24を経て、診療情報記憶装置22に診療情報Xとして、医師ID、患者ID等の医師や患者の特定に必要な情報と共に記録される。

【0012】次に、医師Fは診療を行った結果、診療の専門性、検査、治療設備等の観点から、患者Xを他施設で診療を受けさせた方がよいと判断し、患者Xにその旨を説明し他施設を紹介する。紹介施設は複数(第1の実施例では、B施設とC施設)あり、どの施設で診療を受けるかは患者に委ねることとする。患者から診療情報の提供を望む申し出があった場合には、診療情報を提供する旨を伝える。患者は、自分のICカード18をカードドライブ装置15から取り出し、帰宅又は紹介施設に直接向かう等する。

【0013】一方、医師Fは、入力装置12から診療情報Xの他施設への提供に同意する旨を入力する。例えば、表示画面13を参照して診療情報の提供に関する項目を入力装置12で選択し、提供可能なチェックボタンを有効にする等して提供する意志表示を行う。この意志表示の入力結果は、制御情報記憶装置23に記録される。制御情報記憶装置23には、診療情報記憶装置22の診療情報の管理に必要な情報が、例えば、図2に示すテーブルの形で記録されている。

【0014】図2は、第1の実施例に於いて、診療情報の提供に関する医師の同意の確認に用いるデータの一例を説明する図であり、提供先、提供先の操作者、操作者の操作対象と操作内容に対して、診療情報の扱いに関する事前確認の有無と事前確認内容が記録されている。操作対象とは、提供を依頼する診療情報の種別(例えば、退院時の要約や生化学検査結果等)である。

【0015】データベース制御装置24は、図2に示すテーブルの記録内容に従って、診療情報記憶装置22上の診療情報を制御する。上述の医師Fの診療情報の提供に関する意志表示(同意)の結果、図2の点線で示す枠内の情報が記録される。点線で示す枠内の情報は、B施設又はC施設の医師が各種要約(入院、退院時等の要約)及び検査結果の参照に同意し、その他の情報の提供及び追記には同意しないことを示している。図2に示すテーブルは患者毎に用意され細かな制御が行われる。図2に示すテーブルには、A施設からの操作に関する情報

も含まれている。医師Fは、患者Xの診療及び患者紹介に伴う診療情報の提供に関する一連の作業を終えると、新たな患者の診療にかかる。全患者の診療を終える等、診療端末の利用の終了時、医師Fは、自分のICカード17をカードドライブ装置14から取り出す。

【0016】患者Xは紹介施設としてB施設を選択し、B施設を訪れて医師Gの診療を受ける場合、A施設がB施設に診療情報を提供する手順を説明する。まず、診療端末31は、A施設の診療端末11と同様に、診療に先立って利用者である医師及び患者の本人確認を行う。医師Gは、自分のICカード37をカードドライブ装置34にセットして暗証番号を入力し、患者Xは自分のICカード18をカードドライブ装置35にセットして暗証番号を入力する。

【0017】医師G、患者Xとも本人であると確認後、患者Xは入力装置32を用いてA施設での自分の診療情報のB施設への提供に同意する旨を入力する。A施設の医師Fが意志表示を行ったのと同様に、提供可能というチェックボタンを有効にする等して意志表示を行う。この操作は、患者Xの意志を確認した医師Gが代行してもよい。この入力結果を受けて、端末制御装置36は、A施設のデータベース制御装置24との間でメッセージをやり取りし、診療情報XをB施設に伝送する。この手順の一例を、図1及び図3を用いて詳細に説明する。

【0018】図3は、第1の実施例に於いて、A施設のデータベース制御装置24とB施設の端末制御装置36との間のメッセージの一例を説明する図である。図1に示すステップ42～45は、データベース制御装置24に於ける診療情報の提供手順を制御する処理ステップである。まず、端末制御装置は自分（B施設）の施設名（B施設）及び管理者（医師G）を通知する（51）。データベース制御装置24は、提供先認証ステップ42で提供先が正当な相手か否（不許可施設、他施設のなりすまし等）かを、例えば、図4に示すテーブルを使用して確認する。

【0019】図4は、第1の実施例に於いて、提供先が正当な相手か否かの確認に用いる予め用意されるデータの一列を説明する図である。図4に示すテーブルで示される、診療情報を受け取る施設名（図4に示す提供先）及び管理者（図4に示す操作者）を基に、A施設が提供可能な相手（診療施設）か否かを判定する。又は、必要に応じて予め送付した秘密鍵を用いて相手認証を行う等する。認証方法に関しては、「暗号・認証技術」（電子情報通信学会誌、Vol. 79, No. 2, 第107～114頁）に記載がある。相手先が提供可能な施設の場合、接続許可を通知する（52）。

【0020】接続許可の通知を受けた端末制御装置36は、セッションの初期化を要求する（53）。セッションとは、診療情報データベースを操作する一連の処理の単位であり、第1の実施例では、一人の患者に関するメ

ッセージのやり取りを一つのセッションとして扱う。データベース制御装置24は、実行中のセッションが存在するか否かの確認等を行い、処理のタイミングとして問題なければ了解のメッセージを送る（54）。

【0021】初期化の了解を受けた端末制御装置36は、診療情報の提供を受ける患者XがA施設の自分の診療情報のB施設への提供に同意した旨を通知する（55）。例えば、同意者（患者X）と同意内容（A施設の診療情報X）を含むメッセージを送信する。データベース制御装置24は、患者同意確認ステップ43で受け取った患者同意の内容を確認して問題がない場合、同意完了のメッセージを送る（56）。

【0022】同意完了を受けた端末制御装置36は、患者Xに関するセッションの開始を要求する（57）。データベース制御装置24は、まず、提供元同意確認ステップ44でA施設の診療情報の管理者が診療情報Xの提供を許可しているか否かを確認する。第1の実施例では、制御情報記憶装置23の記録内容を参照し、医師Fの同意が事前にあったことを確認する。提供元同意確認ステップ44での医師Fの同意と患者同意確認ステップ43での患者Xの同意を以て開始を了解するメッセージを送る（58）。

【0023】開始の了解を受けた端末制御装置36は、診療情報Xデータベースの操作対象及び操作内容（ここでは参照）を送る（59）。データベース制御装置24は、診療情報アクセス許可ステップ45で依頼された診療情報を診療情報データベース21から読み出しその内容を送る（60）。メッセージ59及び60は、医師G（診療端末31）が必要な診療情報を受け取るまで繰り返し伝送される。なお、診療情報アクセス許可ステップ45は、制御情報記憶装置23の記録内容を確認しながら処理を行い、図2に示すテーブルで医師Fが同意していない診療情報の提供（具体的には、各種要約及び検査結果以外の診療情報）を拒否する。

【0024】必要な診療情報を受け取ると、端末制御装置36はセッション終了のメッセージを送る（61）。データベース制御装置24は、終了完了のメッセージを送り診療情報を提供する一連の処理を終了する（62）。

【0025】42～44の処理ステップで、接続相手が不正、患者の同意がない、医師Fの同意がない等、処理を失敗した場合には、端末制御装置36に失敗を通知し処理を中断する。即ち、診療情報アクセス許可ステップ45は、医師Fと患者Xの両方の同意がない限り診療情報を提供しない。

【0026】第1の実施例では、患者本人への同意なく診療情報の他施設への提供を防止でき、診療情報に関する患者プライバシーの保護が可能となる著しい効果がある。また、A施設がB施設に診療情報を提供する際に必要となる医師Fの同意確認を、事前（患者XがB施設を

訪れる前)に実行でき、医師Fは、他施設から診療情報の提供依頼がある毎に同意確認の作業を行なう必要がなく、次々と訪れる患者の診療に専念できるという効果がある。更に、患者の意志を尊重し、診療を受ける施設を複数の紹介施設から患者自身が選択できる場合でも、患者が診療施設(B施設)を決定して診療を受ける時点で、患者自身の同意のもとに診療情報の提供を受けることが可能となる。

【0027】(第2の実施例)図5は、第2の実施例で使用する暗証番号の入力装置を備えたカードドライブ装置を説明する図である。第2の実施例では、診療情報XをB施設へ提供する際に必要となる医師Fの同意の確認結果を、患者XのICカード18に記録する構成とする。第1の実施例と同様に、A診療所の医師Fが患者Xを診療し、その診療情報を診療情報記憶装置22に記録する。患者Xを他施設(B施設、C施設)に紹介し診療情報Xを提供する際、提供に関する医師Fの同意の確認結果を、患者XのICカード18に記録する。患者のICカードに医師の同意を、例えば、図6に示すテーブルの形で記録する。

【0028】図6は、第2の実施例に於いて、診療情報の提供に関する患者の同意の確認に用いるデータの一例を説明する図である。図6に示す各項目は、図2に示す項目と基本的に同じである。但し、医師Fが事前確認を行った紹介先施設(B施設、C施設)に関する項目のみとし、記憶容量に制限のある可搬型記録媒体(ICカード)にも記録可能にしている。患者XがB施設で医師Gの診療を受ける場合には、第1の実施例と同様に、医師G及び患者XのICカードをカードドライブ装置にセットした後、診療情報を提供する処理ステップ(42~45)に従い、A施設の診療情報XをB施設に伝送する。但し、提供元同意確認ステップ44では、患者XのICカードに記録された事前確認の結果を用い、A施設と異なる他施設(B施設)から実施し、A施設のデータベース制御装置24とB施設の端末制御装置36との間のメッセージのやり取りを、図7に示す手順により行なう。

【0029】図7は、第2の実施例に於いて、データベース制御装置24と端末制御装置36との間のメッセージの一例を説明する図である。図7に於いて、51~56、及び57~62のメッセージは、第1の実施例の場合(図3)と同じである。第1の実施例で、メッセージ55、56を用いて患者同意確認ステップ43を実施した後、端末制御装置36は、A施設の診療情報の管理者(医師F)が、診療情報XのB施設への提供に同意した旨を通知する(63)。例えば、患者のICカード18からA施設で記録した図6に示すテーブルの内容を読み出し、この内容を含むメッセージを送信する。又は、端末制御装置36でICカードの記録内容から同意の有無を判別して、その結果をメッセージとして送信する。データベース制御装置24は、提供元同意確認ステップ4

4で受け取った医師Fの同意の内容を確認して問題ない場合、同意完了のメッセージを送る(64)。この後の手順は、第1の実施例の場合と同じである。但し、セッション開始の要求のメッセージ57に対する提供元同意確認ステップ44の部分は、既に実行済みなので単に了解のメッセージを58を送る。

【0030】第2の実施例では、診療情報XをB施設に提供する際に必要な医師Fの同意の確認結果を、患者XのICカード18に記録するので、診療情報データベース21の制御情報記憶装置23が不要となる効果がある。更に、診療情報の提供に関する同意を、患者自身がICカードという目に見える誰にでも分かりやすい形で自己管理できるという効果もある。

【0031】(第3の実施例)第3の実施例では、診療情報XのB施設への提供を患者X自身が同意したことを確認する患者同意確認ステップ43を事前(患者XがB施設を訪れる前)に行なう。第3の実施例では、診療情報の提供に関する患者の同意確認を、第1、第2の実施例に於ける医師Fの同意確認と同様に行う。患者Xは、A施設で医師Fから他施設を紹介され、診療情報の提供する旨の話があった時点で、提供に同意するか否かを決定しこの同意内容を制御情報記憶装置23に記録する。

【0032】図8は、第3の実施例に於いて、診療情報の提供に関する患者の同意の確認に用いるデータの一例を説明する図である。制御情報記憶装置23は、患者Xの同意内容を、例えば図8に示すテーブルの形で記録する。図8に示すテーブルは、制御情報記憶装置23に記録される医師Fの同意内容(図2)と同様な形式を持つ。但し、図2のテーブルとは異なる記憶領域に格納され、各々独立して読み出し/書き込みが可能である。第3の実施例では、患者はB施設で診療を受けることにし、B施設への診療情報の提供に同意したものとする。患者が同意した診療情報の提供内容は、図8のテーブルに反映され、点線で示す枠内の情報が設定される。

【0033】A施設からB施設への診療情報の提供は、図1、図3に示した第1の実施例の手順、及びメッセージに従って実現できる。但し、患者Xの同意が事前に済んでいるので、施設Bの診療端末31を用いた患者の本人確認及び同意の意志表示は行わない。具体的には、第1の実施例での、患者XのICカード18のセットや入力装置32を用いた同意の確認等は不要である。また、図3の患者同意に関するメッセージ(56、57)なしに、セッションの初期化後、直ちにセッションを開始できる。セッションの開始の要求(57)を受けたデータベース制御装置24は、先ず、患者同意確認ステップ43を実行する。このステップは、第1の実施例での提供元同意確認ステップ44と同様な手順で、制御情報記憶装置23の記録内容(図8に示すテーブル)を参照し、患者Xの同意が事前に済んでいることの確認で実現される。以下、第1の実施例と同様な手順で提供元同意確認

ステップ44を実行し、患者Xと医師Fの同意を以て開始を了解するメッセージを送る(58)。この後、第1の実施例と同様な手順でメッセージを送受して医師Gは必要な診療情報を受け取れる。

【0034】第3の実施例では、B施設の医師Gは、患者XがB施設に到着する前に診療情報を受け取れるので、例えば必要な検査、治療の準備、ベッドの確保等の受け入れ準備を予め実行でき、患者に対して迅速且つ的確な診療を行える。

【0035】以下に説明するように、第1～第3の実施例の変形は種々可能である。

【0036】第1～第3の実施例でのICカードに代えて、半導体メモリを格納したメモリカード、磁気カード、光カード、フロッピーディスク等の記録媒体も使用できる。病院や診療所で使用されている磁気カードの診察券も使用でき、システムが安価且つ容易に構築できる等の効果がある。

【0037】各診療端末で他の装置での本人確認の結果も使用できる。施設全体の情報管理の担当者による本人確認を別端末で行い結果を各診療端末に伝送し、診療情報の提供の同意確認時にも利用できる。患者が診療施設の受付でICカードを用いて本人確認を行い結果を各診療端末にも伝送できる。安価なシステムが構築でき、診察時に本人確認を実行せず医師は診療に注力できる等の効果がある。

【0038】診療情報データベースに、他の診療施設に提供する診療情報のみを選択的に記録しても良い。診療情報データベースの記憶容量を削減でき、提供不要な診療情報の漏洩を未然に防げる等の効果がある。

【0039】制御情報記録装置に記録した内容を、必要に応じて追加、削除もできる。図2、図6、図8に示す、操作内容から「追記」を削除したり、「消去」を追加してもよく、実際の運用形態に適した最適なシステムを構築できる等の効果がある。

【0040】患者が様態が急変して他施設へ搬送する場合、施設外で患者が倒れて近くの施設に搬送された場合等の緊急時には、患者本人の同意無しに診療情報を提供しても良く、情報を提供したことを記録(ログをとる)し事後に患者の同意を得る。緊急時にも柔軟に対応できる等の効果がある。

【0041】他のシステムと連携したシステムも構築でき、例えば診療情報を提供したことを施設の医事会計システムに自動的に伝送し、保険点数、患者が施設の窓口で支払う自己負担額等の算出に利用できる。診療施設の事務処理の効率化を更にできる等の効果がある。

【0042】提供する診療情報の伝送は、提供元が提供先に書き込み実行してもよい。図3に於いて、セッションの開始後は操作対象と操作内容の通知(59)のみ行い、セッションの終了後、A施設の診療情報データベースからB施設の診療端末に書き込む。第3の実施例に於

いて、A施設で医師と患者の同意が得られた時点で、診療情報を電子メール等でB施設に伝送できる。提供元が提供先に送信するのでなりすまし等の外部からの脅威から診療情報を容易に保護できる効果がある。

【0043】B施設でも診療情報データベースを用意するか、A施設の診療情報データベースに伝送して記録(又は、既存の診療情報に追記)して、B施設からA施設に提供することもできる。

【0044】診療情報を暗号化し診療情報データベースに記録してもよい。医師と患者が異なる秘密鍵(K、L)を持ち、2つの秘密鍵が揃った時点で復号化できる構成とする。診療情報を秘密鍵(Z)で暗号化して記録する。秘密鍵(Z)は患者の秘密鍵(L)で暗号化した後、医師の秘密鍵(K)で暗号化して保管する。診療情報の読み出し(復号化)は、医師の秘密鍵(K)で復号化した後、患者の秘密鍵(L)で復号化した秘密鍵(Z)を用いて行う。公開鍵暗号方式により、診療情報を暗号化した秘密鍵(Z)を保管する方法もある。秘密鍵を医師と患者の公開鍵(R、S)で各々暗号化する。医師は公開鍵(R)で暗号化された秘密鍵(Z)を医師自身の秘密鍵で復号化した後、診療情報を復号化でき、患者は公開鍵(S)で暗号化された秘密鍵(Z)を患者自身の秘密鍵で復号化した後、診療情報を復号化できる。診療情報データベースからの診療情報の漏洩が防止できる等、診療情報の安全性が向上するという効果がある。

【0045】図5に示す、暗証番号入力装置70を備えたカードドライブ装置15を使用して本人確認の実行もできる。医師、患者は、ICカードをセットしたその場で暗証番号を入力でき操作が簡便且つ容易となる効果がある。

【0046】本発明では、提供元診療施設の診療情報の管理者(医師)と患者自身の両方の同意を確認した場合に、診療情報を他の診療施設に提供する。従って、この趣旨を超えない範囲で様々な処理や機能等の追加や変更が可能である。

【0047】

【発明の効果】本発明では、患者本人への同意なく診療情報を他施設に提供することを防止でき、診療情報に関する患者プライバシーを保護できるという著しい効果がある。

【図面の簡単な説明】

【図1】本発明の第1の実施例の地域医療情報システムを説明する図。

【図2】本発明の第1の実施例に於いて、診療情報の提供に関する医師の同意の確認に用いるデータの一例を説明する図。

【図3】本発明の第1の実施例に於いて、データベース制御装置と端末制御装置との間のメッセージの一例を説明する図。

【図4】本発明の第1の実施例に於いて、提供先が正当な相手か否かの確認に用いるデータの一例を説明する図。

【図5】本発明の第2の実施例で使用する暗証番号の入力装置を備えたカードドライブ装置を説明する図。

【図6】本発明の第2の実施例に於いて、診療情報の提供に関する患者の同意の確認に用いるデータの一例を説明する図。

【図7】本発明の第2の実施例に於いて、データベース制御装置と端末制御装置との間のメッセージの一例を説明する図。

【図8】本発明の第3の実施例に於いて、診療情報の提供に関する患者の同意の確認に用いるデータの一例を説

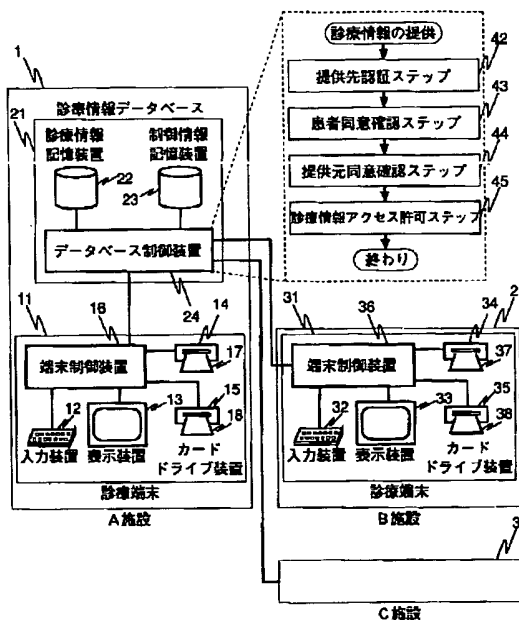
明する図。

【符号の説明】

1…A施設、2…B施設、3…C施設、11、31…診療端末、12、32…入力装置、13、33…表示装置、14、15、34、35…カードドライブ装置、16、36…端末制御装置、17、18、37、38…I/Cカード、21…診療情報データベース、22…診療情報記憶装置、23…制御情報記憶装置、24…データベース制御装置、42…提供先認証ステップ、43…患者同意確認ステップ、44…提供元同意確認ステップ、45…診療情報アクセス許可ステップ、70…暗証番号入力装置、51～64…メッセージ。

【図1】

図1



【図2】

図2

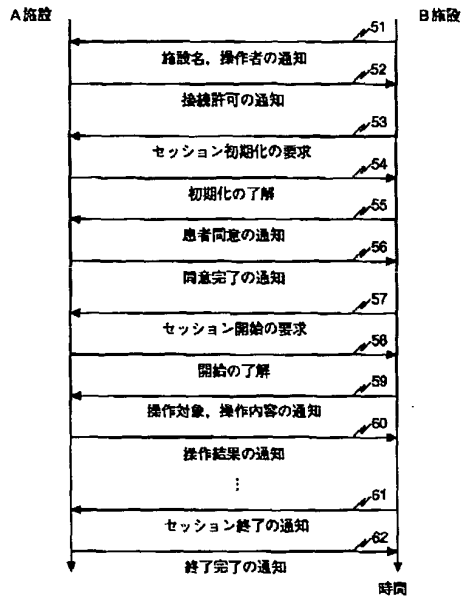
提供先	操作者	操作対象	操作内容	事前確認*1	確認結果*2
A施設	主治医	全情報	参照	○	○
			追記	○	○
	その他の医師	全情報	参照	○	○
			追記		
	その他	全情報	参照	○	○
			追記		
B施設	医師	各種要約	参照	○	○
			追記	○	×
		検査結果	参照	○	○
			追記	○	×
	その他情報	参照	参照	○	×
			追記	○	×
C施設	医師	各種要約	参照	○	○
			追記	○	×
		検査結果	参照	○	○
			追記	○	×
	その他情報	参照	参照	○	×
			追記	○	×
患者宅	医師	全情報	参照	○	○
			追記	○	○
	その他	全情報	参照	○	○
			追記		
その他	全て	全情報	参照	○	×
			追記	○	×

*1: ○は実施、空欄は未実施。

*2: ○は同意する、×は同意しない。

【図3】

図3



【図4】

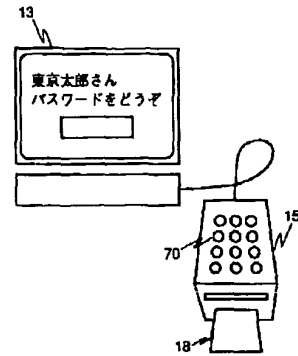
図4

提供先	操作者	接続可否*
A施設	主治医	○
	その他の医師	○
	その他	○
B施設	医師	○
	その他	○
C施設	医師	○
	その他	×
患者宅	医師	○
	その他	○
その他	全て	×

*: ○は可, ×は不可

【図5】

図5



【図6】

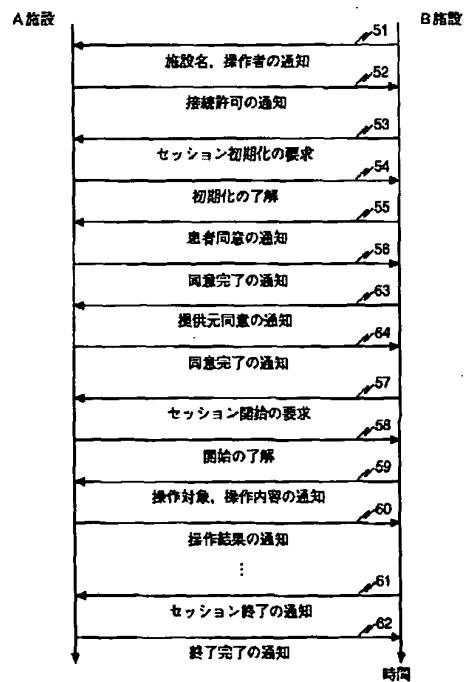
図6

提供先	操作者	操作対象	操作内容	承認内容*1
B施設	医師	各種要約	参照	○
			追記	×
		検査情報	参照	○
			追記	×
		その他情報	参照	×
			追記	×
C施設	医師	各種要約	参照	○
			追記	×
		検査情報	参照	○
			追記	×
		その他情報	参照	×
			追記	×

*1: ○は同意する, ×は同意しない。

【図7】

図7



【図8】

図8

提供先	操作者	操作対象	操作内容	事前確認*1	確認結果*2
A施設	主治医	全情報	参照	○	○
			追記	○	○
	その他の医師	全情報	参照	○	○
			追記	○	○
B施設	医師	全情報	参照	○	○
			追記	○	×
	その他	全情報	参照		
			追記		
C施設	医師	全情報	参照	○	○
			追記	○	×
	その他	全情報	参照		
			追記		
患者宅	医師	全情報	参照	○	○
			追記	○	○
	その他	全情報	参照	○	○
			追記		
その他	全て	全情報	参照	○	×
			追記	○	×

*1: ○は実施、空欄は未実施。

*2: ○は同意する、×は同意しない。